Department of Health & Human Services
Office of the National Coordinator for
Health Information Technology

Update on Privacy and Security Activities

for

National Committee on Vital and Health Statistics

June 15, 2011

Joy Pritts, J.D.
Chief Privacy Officer

HITPC Privacy and Security
Prior Recommendations on Provider Authentication

All entities involved in health data exchange should be required to have digital certificates – Examples of these entities might include:

- Covered entities (health care providers)
  - Retail pharmacies
  - Laboratories
- PHR providers
- Public health entities
- PBMs

Prior Provider Authentication Recommendations--Certificate Authorities

- Multiple credentialing entities will be needed to support issuance of digital certificates given the number of health care entities that will require them – For example, vendors and state agencies, HIOs might be authorized to issue certificates
- Should also leverage existing processes such as the Federal Bridge

Prior Provider Authentication Recommendations--Certificate Authorities

- We recommend that ONC establish an accreditation program for reviewing and authorizing certificate issuers

- This requirement for accreditation should be evaluated in the context of recommendations from the HIT Policy Committee's Governance Workgroup

Revised Certificate Authorities Recommendations

Principles for certificate authorities

- A high level of assurance with respect to organization identity needs to be obtained.
- Multiple competitive sources for digital certificates should be available.
- The certificate should be acceptable to federal agencies, given the frequent need for many providers to exchange information with the federal health architecture.

Revised Certificate Authorities Recommendations

Identified three major approaches:

1. ONC establish an accreditation body, as originally recommended, to supervise organizations that issue certificates (“Certificate Authorities”).
2. Certificate Authorities conform to the best practices of WebTrust and/or European Telecommunications Standards Institute (ETSI).
3. Certificate Authorities must be cross-certified with the Federal Bridge Certificate Authority (either directly or chained up to the FBCA).

Revised Certificate Authorities Recommendations

Certificate Authorities must be cross-certified with the Federal Bridge Certificate Authority (either directly or chained up to the FBCA).

- High level of assurance.
- Multiple competitive sources for certificates.
- Reasonable cost
- One certificate to communicate with private organizations and federal agencies.

Digital Certificate Standards Recommendations

- Generally must conform to the X.509 V3 certificate profile defined in RFC 5280 (May 2008)

Meaningful Use Recommendations

- **Security risk assessment requirement continued from Stage 1**
- **Add requirement that providers focus on encryption at rest (servers and mobile devices) and specifically attest they have addressed this security aspect**
  - Based on fact that encryption is “addressable” security standard and belief that some believe addressable means optional
  - Analysis of breach notification data shows encryption is an issue

P&S Tiger Team

- Future work: Security Framework in light of evolving technology
- Identifying and fill gaps and strengthen Security Rule

Patient Information Matching

Standards Committee has established Patient Matching Power Team to work on issue over the summer.

HITECH Modifications

- NPRM for Accounting of Disclosures published May 31, 2009
- OCR used HITECH plus general rule making authority under HIPAA
- Created right to an “access report” list of people who have accessed electronic health information in a person’s designated record set

Affordable Care Act: Privacy

- NPRM for to CMS share claims data with qualified entities for performance measurement
- NPRM outlines eligibility criteria and operational and governance requirements for entities to become qualified to receive the Medicare data.
- Detailed privacy and security requirements
- Qualified entities not considered business associates of CMS
  - Required to sign data use agreements

Federal Privacy Initiatives

- Baseline federal information privacy bills proposed in Congress
- Based on Fair Information Practices
- Interaction with current sector-specific laws remains an issue (among many others)
- Seems to be some momentum

Questions?